UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,407	09/14/2005	Junbiao Zhang	PU030084	1695

7590 12/28/2009

Joseph S Tripoli
Thomson Licensing Inc
Patent Operations
P O Box 5312
Princeton, NJ 08543-5312

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/549,407
Filing Date: September 14, 2005
Appellant(s): ZHANG ET AL.

Catherine A. Ferguson
Reg. No. 40,877
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 9/29/09 appealing from the Office action mailed on 4/28/09.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Luo U.S. Pub. No. 20030169713 (hereinafter Luo).

As per claim 1 and 5, Luo discloses a method for enabling a client terminal to access a wireless network, comprising the steps of: receiving an access request from the client terminal (Luo: [0037]: access request); redirecting the access request to a local web server via a packet filter for filtering packet traffic (Luo: [0018]: the web-based authentication server; [0037]-[0038]: if the client is in limited state, the client is redirected to the authentication server by the packet traffic filter); requesting from the client terminal, information to establish client terminal access to the wireless network (Luo: [0043]: submitting credential to establish connection to network); activating, in response to the client terminal access information received from the client terminal, a module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user (Luo: [0018]: refer to other accounts that the user has; [0045]: java applet/appropriate parameters used

to connect to wireless network); and authenticating the reconfigured client terminal and allowing access to the wireless network in response to the authentication (Luo: [0045]: grant access after applet is activated).

As per claim 2 and 6, Luo discloses the method of claims 1 and 5 respectively. Luo further discloses wherein the wireless network is an IEEE 802.11 compliant wireless local area network (WLAN), and the client terminal is an IEEE 802.1x compliant client terminal (Luo: [0035]: 802.11x).

As per claim 3, Luo discloses the method of claim 2. Luo further discloses wherein the activating step comprises activating an Active X control/plug-in installed on the client terminal (Luo: [0018] and [0045]).

As per claim 4, Luo discloses the method of claim 2. Luo further discloses wherein the activating step comprises downloading to, and activating in, the client terminal an Active X control/plug-in (Luo: [0045]: java applet).

As per claim 7, Luo discloses a method for configuring a client terminal to provide secure access in a wireless network, comprising the steps of: filtering traffic associated with an HTTP request from the client terminal for access to the wireless network, redirecting the request to a designated web server, and issuing a provider list web page and request from the designated web server to the client terminal for provider selection information to establish an authorized communication (Luo: [0018] and [0037]-[0038]: redirected to the web authentication server if connection is not established).

As per claim 8, Luo discloses the method of claim 7. Luo further discloses wherein the wireless network is an IEEE 802.11 compliant wireless local area network and the client terminal is an IEEE 802.1x compliant client terminal (Luo: [0018]: 802.11x).

As per claim 9, Luo discloses the method of claim 7. Luo further discloses the step of the receiving from the client terminal and communicating to the designated web server information required to establish an authorized connection (Luo: [0042]-[0043]: authentication credential for various authentication methods).

As per claim 10, Luo discloses the method of claim 7. Luo further discloses the step of receiving from the designated web server and communicating to the client terminal access rate information required to establish an authorized communication (Luo: [0018]: create new account; [0043]: provide information to server).

As per claim 11, Luo discloses the method of claim 7. Luo further discloses receiving from the designated web server and communicating to the client terminal access user account creation information required to establish an authorized communication (Luo: [0018]: open new account).

As per claim 12, Luo discloses the method of claim 7. Luo further discloses the step of receiving from the designated web server and communicating to the client terminal access authentication method selection information required to establish an authorized communication (Luo: [0044]: positive acknowledgement page).

As per claim 13, Luo discloses the method of claim 7. Luo further discloses the step of receiving from the designated web server and communicating to the client terminal new account

creation information required to establish an authorized communication (Luo: [0018]: create new account).

As per claim 14, Luo discloses the method of claim 7. Luo further discloses the step of receiving from the designated web server and communicating to the client terminal access user terms and conditions of acceptance information required to establish an authorized communication (Luo: [0018]; [0043]: authentication page).

As per claim 15, Luo discloses the method of claim 7. Luo further discloses the step of receiving from the client terminal and communicating to the designated web server access rate information required to establish an authorized communication (Luo: [0018]).

As per claim 16, Luo discloses the method of claim 7. Luo further discloses the step of receiving from the client terminal and communicating to the designated web server user account creation data required to establish an authorized communication (Luo: [0018]: create new account).

As per claim 17, Luo discloses the method of claim 7. Luo further discloses the step of receiving from the client terminal and communicating to the designated web server user access authentication method selection information required to establish an authorized communication (Luo: [0042]: the authentication page support various user authentication methods).

As per claim 18, Luo discloses the method of claim 7. Luo further discloses the step of receiving from the client terminal and communicating to the designated web server acceptance of the user access terms and conditions required to establish an authorized communication (Luo: [0043]-[0044]).

As per claim 19, Luo discloses the method of claim 8. Luo further discloses whereby the browser program is an ActiveX control (Luo: [0045]: Java applet).

As per claim 20, Luo discloses the method of claim 8. Luo further discloses whereby the browser program is a plug-in (Luo: [0045]: Java applet).

As per claim 21, Luo discloses a mobile terminal, comprising: means for receiving an extended authentication protocol request identification message packet (Luo: [0018]: EAP protocols); means for forwarding an extended authentication protocol response identity message packet (Luo: [0018]: local EAP authentication); means for receiving an extended authentication protocol failure message packet (Luo: [0023]: the connection is limited or blocked due to repeated authentication failure); means for forwarding a web re-direct request (Luo: figure 1: MAP serves as intermediate device to redirect packets between mobile host and plurality of servers; [0018]: web server initiate user-to-network authentication; [0040]: the Web authentication server replies with a short HTTP response message contains a redirect URL pointing to SSL port of itself; [0041]: after receiving the redirect HTTP response, the web browser sends to download authentication page); means for receiving a provider list web page; means for selecting a provider and forwarding said selected provider information (Luo: [0018]: user can refer to authentication server for which the user has account); means for receiving an ActiveX control message to re-configure said mobile terminal (Luo: [0018]: receiving applet); and means for reconfiguring said mobile terminal and establishing authorized communications (Luo: [0018]: applet will be used to provide authentication for consequent communication).

As per claim 22, Luo discloses the method as recited in claim 1. Luo further discloses creating a plurality of operating states, said packet traffic filter receiving wireless local area

network state information from said access point (Luo: [0022]-[0023]: every access point maintains a routing state table to indicate whether packet will be forwarded for respective wireless terminal).

As per claim 23, Luo discloses the method as recited in claim 5. Luo further discloses creating a plurality of operating states, said packet traffic filter receiving wireless local area network state information from said access point (Luo: [0022]-[0023]: every access point maintains a routing state table to indicate whether packet will be forwarded for respective wireless terminal).

As per claim 24, Luo discloses an access point associated with a communications network, comprising: means for forwarding an extended authentication protocol request identification message packet (Luo: [0018]: EAP protocol is used for link layer authentication; [0042]: the authentication server sends the EAP identification message/HTTP response message to prompt user to enter identification information through the access point); means for receiving an extended authentication protocol response identity message packet (Luo: [0043]: sends back the response message/HTTP response containing the credential); means for forwarding an extended authentication protocol failure message packet to a client terminal responsive to a state failure (Luo: [0023]: the state is set to limited if the authentication is failed); means for receiving a re-direct client request from said forwarding means at a packet filter module responsive to said state failure (Luo: [0037]-[0038]: redirect to authentication server if the state is limited); alternative means for receiving a request for access to a communications network at said packet filter module responsive to said state failure (Luo: [0023] routing state table); and means for forwarding a web re-direct request via said packet filter module and for establishing authorized

communications following successful reconfiguration responsive to authentication (Luo: [0023]: the state is normal, access is granted).

As per claim 25, Luo discloses the method of claim 1. Luo further discloses detecting a state failure (Luo: [0023]: detecting whether the state is blocked or limited); and redirecting the access request to a local web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure (Luo: [0037]-[0038]: redirect the request for authentication to authentication server if state is not normal).

As per claim 26, Luo discloses the method of claim 5. Luo further discloses detecting a state failure (Luo: [0023]: detecting whether the state is blocked or limited); and redirecting the access request to a local web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure (Luo: [0037]-[0038]: redirect the request for authentication to authentication server if state is not normal).

As per claim 27, Luo discloses the method of claim 7. Luo further discloses detecting a state failure responsive to receipt of an EAP response identity packet and to receipt of a RADIUS access request reject message (Luo: [0023]: detecting whether the state is blocked or limited); and redirecting the access request to a local web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure (Luo: [0037]-[0038]: redirect the request for authentication to authentication server if state is not normal).

As per claim 28, Luo discloses the method of claim 1. Luo further discloses wherein said information to establish client terminal access to the wireless network comprises provider selection information responsive to receipt of a provider list web page at the client terminal from said local web server (Luo: [0014]).

As per claim 29, Luo discloses the access point of claim 5. Luo further discloses wherein said information to establish client terminal access to the wireless network comprises provider selection information responsive to receipt of a provider list web page at the client terminal from said local web server (Luo: [0014]).

As per claim 30, Luo discloses the mobile terminal according to claim 21. Luo further discloses wherein said provider list web page and said ActiveX control/plug-in are received from a local web server in response to receipt of a web request redirect message from an access point (Luo: [0018]).

As per claim 31, Luo discloses the access point according to claim 24. Luo further discloses wherein said designated web server transmits and ActiveX control/plug-in are received from a local web server in response to receipt of a web request redirect message from an access point (Luo: [0018]).

(10) Response to Argument

Claims 1 and 5:

Appellant mainly argues that the prior art of record does not explicitly disclose "redirecting the access request to a local web server via a packet traffic filter for filtering packet traffic". The examiner disagrees. The prior art of record (Luo) discloses a packet traffic filter

embodied in mobility access point/MAP and packets are filtered based on the state of the mobile host (Luo: [0019]; [0022]-[0023]: a "limited" state means that the mobile host has not been configured or has not been authenticated yet. In this state, the access point should block all frames except those carrying IP configuration packets… HTTP packets between mobile host and Web-based authentication server). On the other hand, MAP redirects access requests depending on the type of packet and frames sent; for instance, IP configuration packet is redirected for first time user that has not been authenticated to a Web Authentication Server/local web server (Luo: Figure 1: MAP serves as intermediate device to redirect packets between mobile host and plurality of servers; [0035]: MAP sends a MOBILE STATE REQUEST message to the Web Authentication Server using the mobile host's MAC address as the index and sets the routing state of the mobile host to "limited"; [0040]: the Web authentication server replies with a short HTTP response message contains a redirect URL pointing to SSL port of itself; [0041]: after receiving the redirect HTTP response, the web browser sends to download authentication page);). As explained in prior office action, the terms used by Appellant may be different from Luo's, Luo nevertheless disclose the steps of filtering packets using packet filter embodied in MAP and redirecting access requests to web authentication server/local web server depending on the state of mobile host.

On the other hand, in response to Appellant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claims 2, 6, and 8:

Appellant argues that the prior art of record does not disclose the limitations of claims 2, 6, and 8 because the IEEE 802.11i standard is currently under development admitted by Luo at [0007]. Although the IEEE 802.11i may have been under development at the time of Luo's invention, IEEE 802.1x and IEEE 802.11 compliant wireless local area networks have been used expensively in the industry (Luo: [0035]: the WLAN card should automatically associate with an MAP using 802.1x/TLS based method).

Claims 3, 19, 20, 30, and 31:

Appellant argues that the plug-in installed on the client terminal as disclosed by Luo functions differently from Appellant's plug-in (or an equivalent client-side program delivered by the web page and installed by the user). The examiner disagrees. Luo discloses configuring mobile host utilizing plug-ins received from web authentication server connected to the MAP (Luo: [0014]: providing Java applet or equivalent plug-ins to mobile host for network configuration). Furthermore, in response to Appellant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim 4:

Appellant's argument on claim 4 is based on argument on claim 3. Therefore, Appellant's argument on claim 4 is traversed based on same rationale set forth above in rejecting claim 3.

Claim 7:

Appellant's argument on claim 7 is based on claims 1 and 5. Therefore, argument is traversed based on explanation set forth above in rejecting claims 1 and 5.

Claim 9:

Appellant argues that Luo does not disclose "designated web server" because it is not an authentication server as disclosed by Luo. However, Luo discloses that the authentication server supports multiple authentication schemes and may require different servers to complete authentication (Luo: figure 1: DNS server, RADIUS server, Web authentication server are shown; [0042]-[0043]: authentication credential for various authentication methods). Furthermore, the claim does not explicitly point out whether the designated web server is an authentication server or a server serving different purpose. Therefore, applicant's argument is traversed.

Claims 10-18:

Appellant argues that the prior art of record discloses, at best, a "possibility," not "inherency". However, the examiner disagrees. Claims 10-18 disclose various steps for opening accounts to establish communication that are well known in the art. Luo discloses the limitations in [0018] by disclosing that the method allows users to open accounts, make one-time payments, or refer the Web-based authentication server to other authentication servers where they have accounts. Therefore, Luo does not simply disclose a possibility, but the ability to perform the steps disclosed in claims 10-18.

Claim 21:

Appellant argues that the prior art of record does not disclose claimed limitations based on 35 U.S.C. 112, sixth paragraph. However, the examiner disagrees. The concept and steps

disclosed in the claims are disclosed by Luo using different terms. Although the terms are not identical, it does not render the claims patentable. Therefore, arguments against claim 21 are traversed based on the rationale provided above.

Claims 22-23 and 25-27:

Appellant mainly argues that the prior art of record does not disclose claimed limitations because they are different. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not clearly recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claims 24 and 31:

Appellant mainly argues that Luo does not disclose means for forwarding extended authentication protocol failure message packets to the client terminal responsive to a state failure and forwarding redirect packets to the designated web server. However, Luo discloses redirecting request packets to other servers that provide different authentication methods when authentication fails (Luo: [0044]: if the submitted authentication credentials are invalid, the Web authentication server generates a negative acknowledgement page and sends the same to the mobile host in an HTTP response message over the SSL. The user can then resubmit the authentication credentials).

On the other hand, Appellant argues that the plug-in disclosed in claim 31 performs differently from Luo's Java applet or equivalent. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon

which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claims 28 and 29:

Appellant's argument on claims 28 and 29 are based on claims 1 and 5. Therefore, argument on claims 28 and 29 are traversed based on above explanation.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Shin-Hon Chen/

Primary Examiner, Art Unit 2431

Conferees:

William Korzuch

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431

Christopher Revak

/Christopher A. Revak/

Primary Examiner, Art Unit 2431